Cisco Firewall Technology

Andrew Mason

ciscopress.com

shortcut

Your Short Cut to Knowledge

Section 2 – Cisco Firewall Technologies

Cisco Firewall Products

Currently, Cisco offers four products that fall into the firewall category: the Cisco IOS Firewall, the Cisco PIX Firewall, the Cisco Firewall Services Module (FWSM), and the Cisco Adaptive Security Appliance (ASA). In this section, we look at the features of each of these firewalls and cover where these are used in a typical business. We also look at the type of hardware available for each technology.

Cisco IOS Firewall is a technology feature that is a part of Cisco Internetwork Operating System, an added benefit because you can use existing hardware at network perimeters to offer true stateful firewalling. If you are looking at using a dedicated appliance, such as the Cisco PIX or ASA, you can also use a Cisco IOS Firewall as a separate layer of security. Because the Cisco IOS Firewall is based on a separate development process than the other firewalls, you can use it to provide a security layer that implements a different firewall technology.

Cisco PIX has been the flagship firewall product from Cisco for more than 10 years. The PIX product has been greatly developed over the years, and the features and functionality of the PIX today make it a world-leading firewall. However, the release of the ASA brings with it massive performance increases, and the addition of a module bay also adds to its feature list. This module bay can currently be populated with an intrusion detection system / intrusion prevention system (IDS/IPS) module or a content security module that offers antivirus, antispam, anti-phishing, and URL-filtering services. The Cisco FWSM is a firewall that sits on a module that fits into the Catalyst 6500 chassis or 7600 router.

Cisco IOS Firewall

The first of the Cisco firewalls we are going to look at is the Cisco IOS Firewall. This “firewall” is not actually a dedicated firewall device, but is firewall functionality included within specific versions of the Cisco IOS Software that runs on Cisco routers. Cisco IOS Software is the operating system Cisco routers and switches operate.

© 2007 Cisco Systems Inc. All rights reserved. This publication is protected by copyright. Please see page 73 for more details

All routers, including the new Integrated Services Routers (ISR), run Cisco IOS Software, and most switches now run Cisco IOS Software and the legacy operating system known as CatOS.

Cisco IOS Software has had a type of firewall included since the early releases, in the form of packet-filtering technology. As previously discussed, this was the first generation of firewall technology. Packet filtering is implemented in Cisco IOS Software by what Cisco calls access lists. Nearly all Cisco routers in service will have access lists configured, because they are flexible in their use. For example, you can use an access list to restrict who can connect to your router over both SSH and HTTPS. For management purposes, you can use an access list to restrict routing updates that are propagated from the router, or received by the router, and, of course, you can use them on an interface to permit or deny specific traffic based on the configuration of the access list.

An early improvement on access lists was the addition of the **established** command. The **established** command is used in an access list as shown here:

```
access-list 100 permit tcp any host 192.168.1.1 eq established
```

This access list permits any TCP connection from anywhere with the destination of 192.168.1.1 as long as it is what is called an established connection. We have covered the TCP three-way handshake earlier in this short cut, and so you know that this type of access list is good to place inbound on an external interface to get around the issue of dynamically allowing return traffic to clients. However, because the router is not tracking the state of the firewall, this does not really fall into the category of a stateful firewall. It is merely filtering packets, albeit ones with a specific flag set in the TCP header.

The first releases of Cisco IOS Firewall improved on the use of the **established** command and implemented a true stateful firewall that ran on a router. This functionality was known as context-based access control (CBAC). We cover CBAC in more detail later in this section.

Routers are located at network perimeters, and the term router itself identifies their functionality: They route packets between networks. You can use them internally within a corporate environment or at the network edge, also known as the network perimeter. Therefore, it can be a good design choice to implement firewalling at this perimeter. There is always a question as to the use and placement of a Cisco IOS Firewall, and it is a good design choice to always provide a separate dedicated firewall such as a Cisco PIX or Cisco ASA. Cisco IOS Firewall does not provide the same level of performance at the same price point as the dedicated Cisco firewalls such as the PIX and ASA. Cisco IOS Firewall does have a considerable resource overhead but can be placed on lower-end perimeter devices where the cost of implementing a standalone firewall is prohibitive. When placing a Cisco IOS Firewall in a busy environment, on a router that performs many core functions, it is always a good idea to monitor the resource utilization on the router to ensure it is within its capabilities.

Features

The main feature of the Cisco IOS Firewall has always been its stateful inspection. Numerous other features (such as URL inspection, intrusion detection, and, more recently, application awareness) have become quite useful, especially for tasks such as blocking or restricting peer-to-peer traffic and instant messaging applications.

We are going to look at some of the main features of the Cisco IOS Firewall. You can access the Cisco home page for the Cisco IOS Firewall at http://www.cisco.com/go/iosfw. At this website, you can find many more design and configuration guides and a wealth of information about the Cisco IOS Firewall.

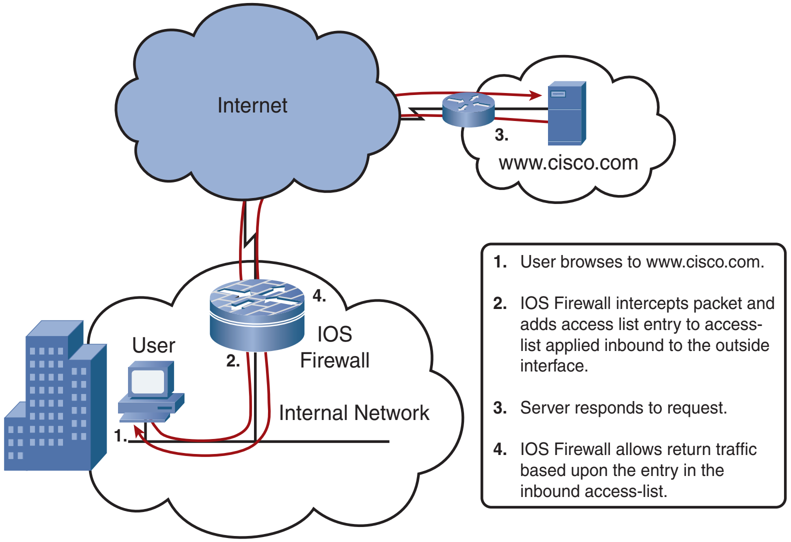
Stateful Inspection

Stateful inspection was the whole reason for the creation of the Cisco IOS Firewall in the first place. Stateful inspection improved on the static packet filters, and the use of the **established** command provided true stateful firewalling. Cisco implemented a technology that they called context-based access control (CBAC). I must admit that learning CBAC can be quite confusing due to the sheer complexity in its offerings. Let’s look at a simple example. We will use the simple network that we looked at earlier: A user wants to access the Internet for web browsing. In the previous sections, we looked at the user using packet filters, and you learned the problems associated with this. You also learned how stateful firewalls help alleviate this issue. We are now going to look at how this is implemented within Cisco IOS Firewall using CBAC.

© 2007 Cisco Systems Inc. All rights reserved. This publication is protected by copyright. Please see page 73 for more details

You can see in Figure 7 that the user is on the inside of the router, which is acting as a firewall as it is running Cisco IOS Firewall. We have an inbound access list applied to the internal interface restricting what can be sent to the outside world. The access list acts as a packet filter, and it allows DNS and web-based traffic.

FIGURE 7
Using Cisco IOS Firewall



1. User browses to www.cisco.com.
2. IOS Firewall intercepts packet and adds access list entry to access-list applied inbound to the outside interface.
3. Server responds to request.
4. IOS Firewall allows return traffic based upon the entry in the inbound access-list.

To configure Cisco IOS Firewall to act in a stateful manner, you have to complete three steps:

1. Configure the firewall inspection rule.
2. Apply the rule to an inbound interface.
3. Apply an access list to the external interface.

© 2007 Cisco Systems Inc. All rights reserved. This publication is protected by copyright. Please see page 73 for more details

NOTE

This is a simple, basic implementation of a Cisco IOS Firewall. For more details about configuring the Cisco IOS Firewall, visit http://www.cisco.com/go/iosfw.

Step 1. Configure the Firewall Inspection Rule

The first step is to configure the firewall inspection rule. You do so by using the **ip inspect** command. The following two lines of code are suffice for this exercise:

```
ip insect name firewall tcp

ip inspect name firewall udp
```

This code creates a set of inspection rules for both TCP- and UDP-based transport layer protocols. It gives these inspection rules the name “firewall”.

Step 2. Apply the Rule to an Inbound Interface

The next step is to apply the inspection rules created in Step 1. The placement of these inspection rules is of utmost importance. We need to apply the inspection rules where connections are initiated, in order for it to know where to apply the stateful inspection. As our traffic is entering the router on the internal interface, we will apply this inspection rule to the internal interface. We also have to specify a direction for the inspection rule. We know the traffic we want to inspect is entering the router, so we apply the inspection rule inbound on the internal interface.

We do so with the following command:

```
ip inspect firewall in
```

With this configuration, the inspection rule named firewall is applied inbound on the internal interface. Therefore, any packets that meet the inspection rule (in our case, all TCP and UDP packets) will be inspected and treated as stateful connections.

© 2007 Cisco Systems Inc. All rights reserved. This publication is protected by copyright. Please see page 73 for more details